APPARATUS, SYSTEM AND METHOD FOR AIRCRAFT SECURITY

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims priority from United States Provisional Patent Application Serial No. 60/482,807 filed June 26, 2003, the entire disclosure of which is incorporated by reference herein.

FIELD OF THE INVENTION

[0002] The present invention relates generally to security mechanisms and more particularly to aircraft security mechanisms.

BACKGROUND OF THE INVENTION

[0003] The airline industry has, for over half a century, transported large volumes of travelers on a daily basis to destinations around the world. One of the primary concerns of the airline industry during this time period has been to maintain the safety of its passengers and aircraft. Over time, the general public, and most airline passengers, developed a positive feeling for airline safety. Statistically speaking, air travel has been considered safer than other presumably safe activities; for example, routinely there have been more people involved in auto or gun related accidents or fires than people involved in aircraft related accidents. The occasional hijacking was not considered a major threat, as most ended without passenger casualties or damage to aircraft.

[0004] The attitude toward air travel forever changed on the morning of Sep. 11, 2001, when the World Trade Center in New York, NY and the Pentagon in Washington, D.C. became the objects of a terrorist attack of previously unimaginable proportions. On

that day, hijackers took over control of four separate aircraft and then managed to personally fly three of those as weapons of mass murder into the buildings, destroying the buildings, surrounding buildings and all three aircraft. The fourth plane crashed into an open field just outside of Pittsburgh following a valiant struggle by passengers to recapture the plane. Tragically, all passengers on all four planes and several thousand people on the ground died that day.

[0005] Following the aftermath of "911", there is now a greater emphasis than ever before on improving airline security to try to prevent hijacking of aircraft. Much of the efforts have been directed to reducing the chances that a successful hijacking may occur, such as by instituting more stringent searches at check-in, by placing armed marshal on flights and by better securing the door separating the passenger and cockpit areas of the plane. These efforts, however, have done little to address the source of the problem, which is hijackers taking over control of an aircraft.

[0006] In view of which, there is seen a need to improve the manner by which the occurrences of hijacking on aircraft can be reduced.

SUMMARY OF THE INVENTION

[0007] In accordance with the present invention, an embodiment comprises a security mechanism for identifying individuals, so as to restrict operation to only those authorized, such as to persons authorized to fly a given aircraft. The security mechanism comprises a controller operable by a user; one or more security devices to identify the user attempting to operate the controller; and one or more monitoring devices to determine whether or not the user identified is authorized to operate the controller.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Fig. 1 is a block diagram of an embodiment of a security system in accordance with the present invention.

[0009] Fig. 2 is a partial schematic, partial block diagram of the system of fig. 1.

[0010] Fig, 3 is a further exemplary embodiment of a rudder control of fig. 2.

[0011] Fig. 4 is a block diagram of an exemplary application of the system of fig. 1.

DESCRIPTION OF THE INVENTION

[0012] In accordance with embodiments of the present invention, an apparatus, system and method is disclosed for restricting the operation of an aircraft, vehicle or other device or system to only authorized personnel. In general, as shown in fig. 1, for this purpose a controller 112 is provided operable by a user, one or more security devices 114, such as biometric readers, is provided associated with the controller 112, one or more monitoring systems 116, such as a computer, is provided in communication with the security devices 114 and one or more control mechanisms 118 is provided in communication with the monitoring systems 116. Any desired biometric characteristics may be utilized for this purpose, such as, for example, fingerprint, retina, facial or DNA characteristics. The one or more biometric readers 114 may be utilized in a variety of different manners, such as being mounted on or integrated within the controller 112 or may be a separate device. The following illustrates exemplary embodiments adapted for aircraft use, such as airplanes or helicopters.

[0013] Fig. 2 is a perspective view of an embodiment in which biometric readers in the form of fingerprint and retina readers 119 and 121, respectively, are associated with

the rudder control 112, i.e., the controller, of an aircraft. In one preferred embodiment, the fingerprint reader 119 is of a type that also incorporates a pulse sensor. In the embodiment shown, the fingerprint/pulse reader 119 may be provided on one or both of the rudder control arms 122a and 122b. The retina reader 121 is shown provided centrally disposed between the two upright rudder control arms 122a/122b. As should be understood, the fingerprint/pulse reader 119 and retina reader 121 may be utilized at other desired locations as well, such as the fingerprint/pulse reader 119 being associated with other components or the retina reader 121 mounted at other locations in the cockpit. The fingerprint/pulse reader 119 and retina reader 121 may be conventional devices, such as any commercially available components, or may be specially manufactured hardware and/or software where desired. Alternatively, as should be understood, other types of biometric sensors may be utilized where desired. In fig. 3 is illustrated another exemplary embodiment of a rudder control 312. In this embodiment, the fingerprint/pulse reader 319 comprises a series of four inward radius portions 330 shaped to accommodate a user's fingers and a thumb reader 332. The remaining portions are the same as that illustrated in fig. 2. As should be understood, the rudder control may comprise other shapes and configurations as well, and should not be construed as being limited to the designs shown in figs. 2 and 3; for example, a single straight arm, circular steering wheel type design, T-shaped, etc.

[0014] In addition, preferably the one or more monitoring systems 116, such as a computer illustrated in fig. 2, is provided in communication with the fingerprint/pulse reader 119 and retina reader 121. The term "computer" as used herein should be broadly construed to comprise any device capable of receiving, transmitting, and/or using information, including, without limitation, a processor, a microprocessor, a personal

computer, a network server, a distributed computing system involving parallel processes over a network, network computing or a mainframe.

[0015] As discussed above, the monitoring system 116 is also preferably in communication with one or more control mechanisms 118 on the aircraft, such as, for example, the rudder control 112, any system controlled by the rudder control 112, the auto pilot control system, a Global Positioning System ("GPS"), such as a GPS chip, located on the aircraft and/or integrated within one or more biometric sensors, or any conventional systems on the aircraft, as examples. The monitoring system 116 may comprise the aircraft's existing on board computer system or may comprise a separate computer system located on the aircraft itself or at designated locations outside of the aircraft, such as an air traffic control center, which is in communication with the on board computer system or directly with the aircraft's security devices 114 and/or control mechanisms 118.

[0016] In addition, the monitoring system 116 may be programmed, such as by authorized personnel, so as to be responsive to data received from the fingerprint/pulse reader 119 and/or retina reader 121 in order to control specific operations of the aircraft, such as designated ones of the aircraft's control mechanisms 118. In some exemplary embodiments, the monitoring system 116 may be preprogrammed so as to grant designated personnel permission to operate the aircraft for specific tasks; for example, granting only the designated pilot and copilot of a certain flight the ability to fly the aircraft, granting designated crew the ability to turn off and/or on the aircraft beacon system, granting designated ground crew and maintenance personnel the ability to service the aircraft, etc. In this manner, different types of permissions may be granted where desired to different categories of personnel. Biometric sensors may be utilized wherever

restrictions may be desired to operate the aircraft; for instance, biometric verification required to fly the aircraft, for operation of the beacon control system or for access into designated areas, for example, via a biometric interlock on doors, panels and/or hatches providing access to any area on the aircraft potentially vulnerable to sabotage, such as, for example, providing access onto the aircraft itself, into cockpit areas and/or for access to storage compartments, such as cargo areas underneath the aircraft, etc. In this and other embodiments, the GPS system may operate by sending positioning information to designated locations, such as ground control, in response to various occurrences on the aircraft, such as, for example, where unauthorized persons attempt to fly the plane, a plane goes off its normal course, etc. An exemplary application of this embodiment is illustrated in the accompanying flow chart of fig. 4, which is described in greater detail below.

[0017] As shown at step 210 in fig. 4, prior to flight, the pilots and crew that are pre-authorized have their fingerprint and retina biometric information loaded into the designated monitoring system 116, such as the airplane's on-board computer. As mentioned above, a separate computer system located on or outside of the aircraft may be utilized as well. The biometric data that is loaded may have been previously taken from the individuals and stored in a database in electronic form, which is then transferred to the plane computer. Alternatively, the biometric data to be loaded may be read from these individuals on site, such as at the time boarding occurs, and then loaded into the on-board computer system at that time. In addition, where desired, a separate biometric check may be performed to verify identity, such as taken from the pilots and crew prior to boarding the plane, such as a fingerprint check that may be compared against stored biometric data for the designated persons, as shown in dotted lines at step 212.

[0018] As shown at step 214, the pilot is required to hold the rudder control 112, so that the pilot's fingerprint/pulse can be detected by the fingerprint/pulse reader 119 and communicated to the monitoring system 116 to verify identity. An authorized pilot will be able to fly the aircraft, as shown at step 216. Otherwise, as shown at step 218, the rudder control 112 will not function properly and the individual will not be able to fly the plane; for example, in one embodiment, the monitoring system 116 will kick back to auto-pilot mode, as shown at step 220. The term "fly" as used herein should be broadly construed to refer to any phase of an aircraft flight, starting up of the aircraft, movement of the aircraft from a fixed position, take-off or landing of the aircraft, taxiing of the aircraft as well as in the air flight. Accordingly, in other exemplary embodiments, where the aircraft is on the ground, for instance, the monitoring system 116 may operate to prohibit takeoff where an unauthorized pilot is detected, for example, by failing to turn on engines, locking of the rudder control 112, etc. Further, where an unauthorized person may place their hand on the rudder control 112 in order to try to fly the airplane, the monitoring system 116 may also communicate that information to designated authorities, such as, for example, via an unauthorized pilot notification or a disaster alert signal sent to ground control, as shown at step 222. The monitoring system 116 may also at the same time send the unauthorized person's biometric data to designated authorities, as shown at step 224, so that a subsequent biometric check may be performed to uncover the identity of that individual. In this embodiment, the pulse sensor of the fingerprint/pulse reader 119 operates to detect further information about the condition of the individual holding the rudder control 112, such as whether or not there is the presence of a pulse, to signify that the hand placed on the rudder control is of a live individual, or if there is a rapid or irregular pulse, such as to signify that the individual is in a distressed state. The

monitoring system 116 can be programmed to notify authorities, such as ground control, if any such unusual pulse reading occurs, such as, for example, via a distressed pilot notification or a disaster alert, as shown at step 226.

[0019] In addition, the retina reader 121 can also be used in this embodiment as an additional level of security , such as to communicate with the monitoring system 116 so as to authorize engagement or disengagement of the auto-pilot. For example, the retina reader 121 can verify whether an authorized pilot is in his or her seat, and control subsequent operations based that information, where desired, such as to allow disengagement of the auto-pilot, as shown at steps 228-232. Other suitable types of biometric devices may be utilized as well where desired in place of the retina reader 121; for example, a heat signature device or a camera located in the seat of the pilot rather than a retina reader. In certain embodiments, retina reader 121 can comprise one or more commercially available cameras adapted for taking a biometric read of the retina of designated persons at specified times. For example, the camera can of a type activated to take a biometric read anytime there is motion sensed. For instance, the camera can be mounted in the cockpit area and operated to take a retina read anytime there is movement by the pilot. In addition, that same camera, or another camera, can be provided to take a photograph of the designated person at the same time a retina read is taken. Multiple cameras may also be used where desired, such as for the pilot and copilot, etc. In addition, in this and other embodiments, the camera can also be activated so as to take a photograph of the designated persons at other desired times, such as when an unauthorized person attempts to take the controller or access particular areas, an irregular pulse is detected or any other distressed condition is detected. The photograph, along with any other desired information, may then be transmitted to desired locations, such as

via satellite, cellular or independent transmitter, as examples. Some examples of the desired locations include, but area not limited to, the airlines, as mentioned above, the Department of Defense and/or Department of Homeland Security.

[0020] In some embodiments, it may be desired to grant permission to certain additional persons as a matter of course or in emergency situations to have limited or full authority to operate the aircraft who originally did not have that authority. For instance, in certain circumstances, for example, such as where any crew become ill or incapacitated during a flight, it may be desired that authority to operate a given aircraft be granted to additional persons, such as any off duty crew or any passenger pilots on the aircraft. In such situations, a biometric check can be implemented to verify identity of the additional persons before any authority to operate the aircraft will be given. The biometric check can be performed on the aircraft and compared against stored biometric information contained either on the aircraft, such as contained in the on-board computer, or any database located outside of the aircraft, such as a database kept by designated authorities, such as by individual airlines, the airline industry or a central reporting database, as examples. The biometric check can be done by utilizing a separate biometric device on the aircraft, or by using any of the existing biometric devices mentioned above, such as the fingerprint/pulse reader 119 and/or retina reader 121.

[0021] As should be understood, the embodiments discussed above can be susceptible to many different modifications or variations. For example, it should be understood that any number of security devices may be used in connection with embodiments of the present invention, and with any number being biometric readers. For instance, in the illustrated embodiment, one or more biometric readers may be utilized

where desired, and the biometric readers may be of any desired type, such as a fingerprint/pulse reader and/or retina reader as shown or any other desired types of biometric reading devices. In addition, in certain embodiments, it may be desired that there be a combination of biometric and nonbiometric type security devices, or that no biometric type security devices be used. In addition, the term "controller" as used herein should be broadly construed to comprise any suitable type of device, system or method for regulating operation, such as a rudder control of any desired shape, as mentioned above, a keyboard, trigger, buttons, tracking ball, single or dual joystick, lever, wheel, etc. Further, while the illustrated embodiment is described in relation to aircraft, it should be understood that embodiments may also comprise other types of apparatus or systems as well, including vehicles, such as, for example, military vehicles, commercial vehicles(e.g., trains, buses, trucks, taxi cabs, etc), private vehicles(e.g. passenger cars), or any desired products or equipment, such as controls for nuclear reactors or military weapons, computer terminals, firearms, etc. The embodiments of the present invention may be implemented using hardware or software or any combination of the two where desired. Various embodiments may also be implemented using commercially available technology. Accordingly, it is intended that the invention not be limited to the specific illustrative embodiments, but be interpreted within the full spirit and scope of the appended claims and their equivalents.